Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter

Office of the Chief Information Security Officer
September 2008 | Volume 2, Issue 9

Firewalls

WHAT IS A FIREWALL, AND WHY SHOULD I USE ONE?

A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. Firewalls add a layer of protection by blocking unauthorized and potentially dangerous data from entering your computer or network. Firewalls are especially critical for users who have an *always on* connection to the Internet.

Some users may think that data residing on their computer is not valuable and, therefore, feel that a firewall is not necessary. However, even small pieces of information can be obtained by the hacker and used to steal identities and other personal data. In addition, hackers may be interested in taking over your computer to store illegal materials or launch other attacks that can leave a trail back to your computer. Once a hacker gets access to your computer, the intruder may have access to resources and data stored on your machine.

WHAT DOES A FIREWALL PROTECT ME FROM?

Firewalls can help protect your data and computer by blocking:

- Unsolicited traffic/malware from coming into your computer or network
- Traffic from known malicious computers
- Specific traffic you don’t want leaving your computer or network
- Programs, protocols, and ports that you specify
- Attempts to access or attack your computer

Firewalls can also log activity, and these logs should be reviewed periodically to identify any anomalous or unexpected activity.

WHAT TYPE OF FIREWALL SHOULD I USE?

There are two types of firewalls: hardware and software. A hardware firewall is usually an external device that sits between your computer and your connection to the Internet. A software firewall (also known as a personal firewall) runs directly on your computer. This firewall is the most common type for home users.

WHAT SHOULD I KNOW BEFORE INSTALLING AND ENABLING A FIREWALL?

Before installing and enabling a firewall, read the documentation carefully to ensure proper configuration. A properly configured firewall can save you hours of recovery or rebuilding of data.

Consider the following when installing a firewall:

- Allow only the traffic that you need.
- Enable the *automatic update* feature if one exists, and periodically check the firewall vendor's web site for the latest software updates.
- Enable the logging feature, and review the logs regularly.
- Change the default *administrator* account (if available) and password.
- Disable the remote management option (if available).

A firewall is a very valuable tool for protecting your data and your computers, but it must be selected, installed, configured, monitored, and maintained effectively to do its job. Please note that, although firewalls can block intruders, viruses, or unwanted traffic from getting into your computer, using a firewall is not a complete solution to security. Firewalls should be used along with anti-virus, anti-spyware, and anti-spam software as part of a defense-in-depth strategy for protecting your computer from various forms of malware (viruses, worms, Trojans, etc.), hackers, and others who want your data or your computer for illegal or malicious purposes.

Remember: Cyber Security is Your Responsibility. Always apply safe cyber security practices to protect the data on your computer or network.

ADDITIONAL RESOURCES

To learn more about firewalls, please visit the following sites:

- MS-ISAC – Beginners Guide to Firewalls: **www.cscic.state.ny.us/localgov/#download**
- US-CERT – Understanding Firewalls: **www.us-cert.gov/cas/tips/ST04-004.html**
- How Stuff Works – Firewalls: **computer.howstuffworks.com/firewall.htm**
- Firewalls for Dummies: **www.dummies.com/WileyCDA/DummiesTitle/Firewalls-For-Dummies-2nd-Edition.productCd-0764540483.html**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.

For more information on Internet security, please visit the SecureTexas website – **www.dir.state.tx.us/securetexas**. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC **www.msisac.org**

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM **www.us-cert.gov**

Distributed by: DIR Secure Texas **www.dir.state.tx.us/securetexas**